ARTICLE IN PRESS

Ad Hoc Networks xxx (2013) xxx–xxx

Contents lists available at SciVerse ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

On the tradeoff between altruism and selfishness in MANET trust management

Jin-Hee Cho [a,*], Ing-Ray Chen [b]

[a] Computer Scientist Computational & Information Sciences Directorate (CISD), U.S. Army Research Laboratory (USARL), 2800 Powder Mill Rd, Adelphi, MD 20783, United States

[b] Department of Computer Science, Virginia Tech, 7054 Haycock Road, Falls Church, VA 22043, United States

ARTICLE INFO

Article history:
Received 1 August 2012
Received in revised form 19 March 2013
Accepted 6 May 2013
Available online xxxx

Keywords:
Altruism
Selfishness
Demand and pricing theory
Mobile ad hoc networks
Trust management

ABSTRACT

Mobile ad hoc and sensor networks may consist of a mixture of nodes, some of which may be considered selfish due to a lack of cooperativeness in providing network services such as forwarding packets. In the literature, existing trust management protocols for mobile ad hoc networks advocate isolating selfish nodes as soon as they are detected. Further, altruistic behaviors are encouraged with incentive mechanisms. In this paper, we propose and analyze a trust management protocol for group communication systems where selfish nodes exist and system survivability is highly critical to mission execution. Rather than always encouraging altruistic behaviors, we consider the tradeoff between a node's individual welfare (e.g., saving energy to prolong the node lifetime) vs. global welfare (e.g., achieving a given mission with sufficient service availability) and identify the best design condition of this behavior model to balance selfish vs. altruistic behaviors. With the system lifetime and the mission success probability as our trust-based reliability metric, we show that our behavior model that exploits the tradeoff between selfishness vs. altruism outperforms one that only encourages altruistic behaviors.

Published by Elsevier B.V.

1. Introduction

Most existing works on trust management in mobile ad hoc networks (MANETs) in the presence of selfish nodes encourage cooperative behaviors while discouraging selfish behaviors of participating nodes, so as to achieve a system goal such as high service availability. A common solution is to isolate selfish nodes as soon as they are detected and to reward altruistic nodes with incentive mechanisms to encourage cooperation. Many MANET applications such as disaster management, rescue missions, and military tactical operations often require multi-hop communications (e.g., multicast or broadcast) without the presence of a trusted infrastructure in an environment where resources (e.g., bandwidth, memory, computational power, and energy) are severely constrained. In such applications, encouraging only altruistic behaviors may lead to a short system lifetime span. This is because altruistic nodes may die quickly due to energy depletion, thus possibly causing a system failure as there are not enough nodes remaining in the system to continue service. This is especially detrimental to systems designed to prolong the system lifetime for successful mission execution.

Thomas et al. [1] studied system performance in this scenario, and claimed that there must be a tradeoff between energy saved by selfish nodes and service availability provided by cooperative nodes. However, no analysis of the tradeoff was given. Papadimitriou [2] described these two conflicting goals (i.e., the local goal of a selfish node to save its energy vs. the global goal of an altruistic node to provide high service availability) with the term "the price of anarchy." The price of anarchy was defined as

* Corresponding author. Tel.: +1 301 394 0492 (J.-H. Cho), tel.: +1 703 538 8376 (I.-R. Chen).

E-mail addresses: jinhee.cho@us.army.mil (J.-H. Cho), irchen@vt.edu (I.-R. Chen).

1570-8705/$ - see front matter Published by Elsevier B.V.
http://dx.doi.org/10.1016/j.adhoc.2013.05.004

the performance difference between a system run by an all-knowing benign dictator who can make right decisions to optimize system performance vs. a system run by a selfish anarchy.

We advocate that, as in other engineering fields, there should be a tradeoff between system survivability and service availability in terms of these two conflicting goals. As Thomas et al. [1] indicated, each node can cognitively make a decision for its own interest as well as for global interest such as system goals. In this paper, we address this problem by proposing and analyzing a behavior model that exploits the tradeoff between selfishness vs. altruism for system survivability for a cognitive mission-driven group communication system (GCS) in MANETs based on the concept of cognitive networks. Each node has intelligence to adapt to dynamically changing MANET environments through a learning process, thereby adjusting its altruistic vs. selfish behaviors in response to future dynamics. We seek to identify the optimal design settings that maximize the system lifetime and consequently the mission success probability while satisfying performance requirements such as service availability.

We adopt the demand and pricing (DP) mechanism originally derived from economics [3] by which a node decides whether it should behave selfishly or altruistically based on the balance between individual welfare (i.e., saving energy) and global welfare (i.e., providing services). A node's decision may depend on its own energy level, 1-hop neighbors' selfishness levels (i.e., to judge whether the system still has sufficient resources even if the node is selfish), and the degree of mission importance (i.e., to judge whether a node's selfish behavior would have a significant detrimental impact on mission success). In the literature, social scientists have addressed the tradeoff between local/individual utility and global/collective interest in the area of collaboration theory using the trust concept in groups, teams, and organizations [4]. However, no prior work exists to address this tradeoff in the context of networking environments.

Many routing protocols for MANETs have been developed to isolate selfish nodes and to encourage collaboration among participating nodes [5–12]. Das et al. [5] proposed a new credit-based system for MANETs where each node has a unique IP address. Djenouri et al. [6] demonstrated an optimization mechanism to improve quality-of-service (QoS) by alleviating the effect of selfish nodes. Kargl et al. [7] developed a mechanism to detect selfish nodes. Wang et al. [8] devised an efficient incentive mechanism to encourage cooperative behaviors. Zhao [9] and Yan and Hailes [10] proposed game theoretic approaches to encourage cooperativeness. Miranda and Rodrigues [11] proposed an algorithm to discourage selfish behaviors based on a fair distribution of resource consumption. Different from the above work [5–11], Zhang and Agrawal [12] reversed the common intuition about selfish nodes; they found the positive aspect of having selfish nodes in terms of traffic reduction, and identified the optimal number of selfish nodes. Except [12], all prior works above emphasize the disadvantages of having selfish nodes in MANETs. Our work in this paper is different from all above works [5–12] in that we investigate and identify the best balance between individual benefit via selfish behaviors vs. global interest via altruistic behaviors so as to prolong the system lifetime for successful mission execution.

A number of routing protocols have been proposed based on the concept of trust (or reputation) to isolate selfish nodes [13–19]. Refaei et al. [13] proposed a reputation-based mechanism using various types of reputation functions and identified the optimal scheme that reduces false positives and isolates selfish nodes. He et al. [14] also proposed a reputation-based trust management scheme using an incentive mechanism, called SORI (Secure and Objective Reputation-based Incentive), to encourage packet forwarding and discourage selfish behaviors based on reputation propagation by a one-way hash chain authentication. Pisinou et al. [15] devised a secure AODV (Ad hoc On Demand Distance Vector) based routing protocol for multi-hop ad hoc networks to find a secure end-to-end route free of black hole attack, route injection, and selfish nodes. Soltanali et al. [16] proposed a distributed mechanism to deal with selfish nodes as well as to encourage cooperation in MANETs based on a combination of reputation and incentives. Moe et al. [17] proposed a trust-based routing protocol based on an incentive mechanism to discourage selfish behaviors, using a hidden Markov model (HMM) to quantitatively measure the trustworthiness of nodes. Adams et al. [18] proposed a node-centric reputation management scheme that considers feedback of a node's behavior in generating a reputation index in order to determine trustworthiness of its peers before establishing IPSec security associations. Velloso et al. [19] proposed a human-based model which describes a maturity-based trust relationship between nodes in MANETs.

These trust-based schemes cited above [13–19] in general aim to isolate or discourage selfish behaviors of participating nodes. Moreover, the trust metric used frequently does not adequately consider unique properties of trust in a MANET environment, including subjectivity, asymmetry, incomplete transitivity, dynamicity, and context-dependency [20]. Our work takes these properties into consideration and adopts a trust metric that reflects both social trust derived from social networks and QoS (quality-of-service) trust derived from communication networks. Our interest is not so much in isolating selfish nodes but in quantifying the tradeoff between individual and global welfare, allowing each node to adapt to network dynamics and node status.

In game theory (or Nash equilibrium), an entity is assumed to be rational to maximize its own payoff, which is usually regarded as selfish. Most existing work used rewards or incentives to entice cooperativeness and discourage selfishness so that each entity makes moves to obtain the best individual payoff. In this work, we reveal that each node can actually dynamically adapt its behavior to achieve both its individual goal and global goal. A behavior model is proposed modeling an entity's altruism vs. selfishness behavior such that when it has a global view to execute a mission successfully which requires its longevity, it can be temporarily selfish to save its energy so it can contribute to successful mission execution. While traditional game theoretic approaches are solely based on a node's rationality, being selfish or cooperative to maximize

Please cite this article in press as: J.-H. Cho, I.-R. Chen, On the tradeoff between altruism and selfishness in MANET trust management, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.004

its payoff, our approach proposes an adaptive strategy of "altruistic selfishness" (providing service to increase trustworthiness for not being isolated from the network) or "selfish altruism" (saving energy to prolong the node lifetime so as to contribute to successful mission execution) to best balance altruistic behavior vs. selfish behavior.

Researchers have taken economic perspectives in modeling network behaviors and solving practical service problems in telecommunication systems [21–27]. Marbach and Qiu [21] took a market-based approach to encourage cooperation among nodes in MANETs by charging the service for relaying data packets. Aldebert et al. [22] analyzed residential demand by traffic destination using the demand and pricing (DP) theory. Yilmaz and Chen [23] utilized the DP theory to model an admission control algorithm with the goal of revenue optimization with QoS guarantees in wireless cellular networks. Rappaport et al. [24] analyzed a consumer survey to estimate household demand for wireless internet access. Kamioka and Yanada [25] used the DP theory to explain the relationship between the service demand of source nodes and the service supply of relay nodes. Xi and Yeh [26] investigated pricing games in multi-hop relay networks where selfishly and strategically behaving nodes charge their service and accordingly route their traffic. Chen et al. [27] proposed a fair-pricing focused incentive mechanism to encourage cooperation in MANETs. Different from the works cited above [21–27], we use the DP theory to model the selfish and altruistic behaviors of a node in MANETs.

Recently trust has been applied to security applications such as secure routing or intrusion detection in MANETs [36]. Bao et al. [34] proposed a cluster-based hierarchical trust management protocol for large-scale wireless sensor networks (WSNs) to effectively deal with selfish or malicious nodes. They tested their proposed protocol to maximize security application performance in secure routing and intrusion detection. Fung et al. [35] proposed Dirichlet-based trust management to measure the level of trust among intrusion detection systems according to their mutual experience including the degree of acquaintance between two entities. However, these works [34,35] do not consider the balance between a node's selfish behavior and altruistic behavior to maximize the system goal.

Different from existing work cited above, the goal of this work is not to use the proposed behavior model to determine whether to trust a node or not. Our goal is to demonstrate that when nodes can balance altruistic behavior (i.e., providing high service availability) vs. selfish behavior (i.e., saving energy) in accordance with the DP theory, the system reliability can be improved compared with pure altruistic or pure selfish behaviors.

The contributions of this work are as follows. First, we develop and analyze a selfishness vs. altruism behavior model for a mission-driven GCS in MANETs where nodes may behave selfishly. We use the DP theory to quantify the conflicts between individual welfare and global welfare, and identify the condition to best prolong the system lifetime for successful mission execution while satisfying performance requirements. Second, we propose a composite trust metric encompassing social trust for sociability and QoS trust for performance capability. This composite trust metric allows us to cover a wide range of GCS applications with humans in the loop carrying communication devices to execute a mission assigned. Third, we develop a reliability metric, called the mission success probability, to predict the degree of successful mission completion for a trust-based GCS. This metric uniquely reflects the impact of trust management on system reliability. Fourth, we develop a mathematical model to describe the proposed GCS based on hierarchical Stochastic Petri Nets (SPN) [37], allowing optimal conditions to be identified to answer what-if types of questions for operational and environmental condition changes. Fifth, we demonstrate that our DP behavior model exploiting the tradeoff between selfishness vs. altruism is capable of maintaining an acceptable trust level while achieving a high mission success probability and a prolonged system lifetime, compared to both a purely altruistic system and a purely selfish system.

This paper significantly extends our preliminary work published in [32]. Compared to [32], this paper has new contributions including: (1) a new composite trust metric (Section 2.3); (2) a new trust-based reliability metric to predict the mission success probability (Section 3.3); (3) an analysis comparing the DP behavior model with the two baseline behavior models in terms of the trust level obtained, the percentage of cooperative nodes obtained, and the trust-based reliability assessment; and (4) an analysis of the DP behavior model by varying key design parameters to investigate its usefulness in practice.

The rest of this paper is organized as follows. Section 2 describes the system model, including the trust protocol description, assumptions, trust metric, energy model, and behavior model. Section 3 develops a performance model based on hierarchical SPN subnets. In addition, Section 3 discusses and defines the mission success probability as the trust-based reliability metric to predict trust-based system survivability. Section 4 analyzes numerical results obtained through the evaluation of our SPN performance models. In particular, we perform a comparative analysis of the DP behavior model against a solely altruistic model and a solely selfish model. We also investigate the sensitivity of our results with respect to critical design parameters. Finally, Section 5 concludes the paper and outlines future work.

2. System model

2.1. Trust-based cognitive networks for MANETs

Due to the unique characteristics of MANETs and the inherent nature of the unreliable medium in wireless networks, trust management for MANETs should encompass the following trust concepts: it should be dynamic and account for uncertainty; it should be context-dependent, and subjective, and not necessarily transitive or reciprocal. To reflect these unique trust concepts in MANETs, trust management for MANETs should consider the following design features: trust metrics must be customizable, evaluation of trust should be fully distributed without reliance on a cen-

Please cite this article in press as: J.-H. Cho, I.-R. Chen, On the tradeoff between altruism and selfishness in MANET trust management, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.004

tralized authority, and trust management should cope with dynamics and adverse behaviors in a tactical MANET [36].

Cognitive networks are able to reconfigure the network infrastructure based on past experiences by adapting to changing network behaviors to improve scalability (e.g., reducing complexity), survivability (e.g., increasing reliability), and QoS (e.g., facilitating cooperation among nodes) as a forward looking mechanism [1]. We use this concept of cognitive networks to introduce intelligence into each node to adapt to changing network conditions, such as a node's selfish behavior, node failure or mobility, energy exhaustion of a node, or voluntary disconnection for energy savings.

In the initial network deployment, we assume that there is no predefined trust. Without prior interactions, the initial bootstrapping will establish a shallow level of trust based only on indirect information (e.g., reputation from historically collected data or recommendation by third parties) and authentication by a challenge/response process (e.g., public key authentication). Over time, participating nodes will establish a stronger trust level with more confidence based on direct or indirect interactions and changing operational and environmental network conditions. Our trust management protocol allows each node to evaluate the overall trust of other nodes as well as to be evaluated by other nodes based on two factors, social trust and QoS trust. Social trust includes trust properties for "sociable" purposes while QoS trust includes QoS properties for mission execution purposes [20].

Trust decays over time without further updates or interactions between entities. Node mobility also hinders continuous interactions with other group members, lowering the chances of evaluations of each other in the group. This includes cases such as a node moving towards other areas causing its disconnection from the current group, leaving a group for tactical mission reasons, and either voluntary disconnection for saving power or involuntary disconnection due to terrain or low energy. In addition, when we use the concept of *web of trust* [28], we obtain a certain degree of trust based on the length of the web of trust. For example, when the length of the trust chain is 4, e.g., A trusts B, B trusts C, C trusts D, and D trusts E, then, A may trust E. However, the longer the trust chain is, the more is the decay in the degree of trust [28]. Note that we use direct trust relationships when trust information is passed from A to E. Particularly, we call referral trust from A to D (i.e., A–B, B–C, C–D) and functional trust from D to E (i.e., D–E) [31]. Referral trust is the one used to pass references from A to D while functional trust is the one used to obtain the trust information of a target node from D that directly knows E.

Our target system is a mission-driven GCS in military tactical MANETs where a symmetric key, called the group key, is used as a secret key for group communications between group members [20]. Upon a node's disconnection from the group, the system generates and redistributes a new key so that non-member nodes will not be able to access a valid secret group key. Nevertheless, each group member keeps old trust information even for non-member nodes so that the information can be reused for future interactions, preventing a new comer attack.

2.2. Assumptions

We assume that the GCS is in a MANET environment without any centralized trusted entity in which nodes communicate through multiple hops. Nodes have different levels of energy, thus reflecting node heterogeneity. Each node periodically beacons its identification (ID) and location information to its 1-hop neighbors so that node failure or node leaving events can be easily detected by 1-hop neighbors to support our trust protocol design. We contrast our design with an efficient beacon-less routing protocol [44] which uses a relay node to forward a beacon message to avoid redundant dissemination of the beacon message to the network. Instead of disseminating a beacon message to the entire network, we limit beaconing to only 1-hop neighbors so that 1-hop neighbors can gain trust evidence towards a node based on beacon messages received. Accordingly rekeying is done immediately upon every membership change, and all member nodes are periodically aware of other nodes' location and their ID in the network. Due to the goal of the GCS that a mission should be completed based on the collaboration or cooperation of nodes in the network, we consider one group with group members that intend to pursue and successfully complete an assigned mission. Involuntary disconnections or reconnections caused by network topology changes (e.g., network split or merge due to node mobility or failure) are implicitly considered by a node's join or leave and the corresponding rekeying cost is considered in calculating energy consumption, as shown in Section 2.4. A node's disconnections or reconnections are incorporated in calculating trust values of a node based on "closeness" component, as discussed in Section 2.3.

We assume that mobile devices are carried by humans such as dismounted soldiers. We model group member join and member leave operations as common events for a GCS. Upon every membership change due to join/leave, a rekeying operation will be performed to generate a new group key based on a distributed key agreement protocol such as GDH (Group Diffie Hellman) [38]. We assume that nodes move randomly in a MANET environment. The energy consumption rate of a node depends on its status. The energy model is described in Section 2.4. A node's selfishness vs. altruism behavior is modeled by a behavior model. The behavior model is described in Section 2.5. The mobility model, energy model and behavior model are input to the trust management protocol.

We assume that a node's trust value is being evaluated based on direct observations (e.g., packet dropping) as well as indirect observations. Indirect observations are recommendations obtained from 1-hop neighbors with the highest trust values. If sufficient recommenders cannot be found, recommendations from all 1-hop neighbors can be used. Each node disseminates a status exchange message containing its ID and its trust evaluation information toward its 1-hop neighbors (based on direct observations) periodically. This will enable each node to compute trust values of other nodes considering the original recommendations from the 1-hop neighbors of a target node as well as the reliability of the path that the trust information is obtained. It is assumed that each node can observe behav-

Please cite this article in press as: J.-H. Cho, I.-R. Chen, On the tradeoff between altruism and selfishness in MANET trust management, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.004

iors of 1-hop neighbors and compute interested trust component values based on the direct observations using a reputation monitoring mechanism pre-installed such as Watchdog or Pathrater [33]. When each node receives the status exchange messages, it can calculate trust based on desired trust availability and required path reliability. Trust availability is the probability that a target node exists within an n-hop distance from the evaluator's location where n refers to the length of a trust chain used. That is, as n increases, trust availability increases. On the other hand, when a target node is found within n hops from the evaluator's location, the reliability of a route taken by referral trust recommenders (called path reliability) to pass the trust information (recommendation) from the functional trust recommender of the target node will decrease. We calculate the path reliability by the product of referral trust values of all referral trust recommenders where the referral trust value is measured by unselfishness (a trust component considered in our trust management protocol), measuring the protocol compliance of a referral trust recommender. We will discuss path reliability in more detail in Section 2.3. As n increases, the path reliability decreases. Based on this tradeoff, each node cognitively and adaptively adjusts the length of its trust chain in order to collaborate with more nodes to achieve the desired trust availability while maintaining the required path reliability.

We consider the presence of outside attackers. We assume that existing prevention techniques such as encryption, authentication, or rekeying inhibit outsider attacks. We consider the presence of both selfish nodes and compromised nodes among legitimate group members. We distinguish selfish nodes from compromised nodes in that a selfish node can adjust its status from selfish to unselfish or unselfish to selfish depending on the network conditions while a compromised node performs packet dropping attacks and stays selfish continuously. We model the behaviors of a selfish node by the DP theory, as described in Section 2.4.

2.3. Trust management protocol

We consider a trust metric that spans two aspects of the trust relationship. First, social trust [30] will be evaluated through social networks to account for social relationships. We consider *closeness* for social trust where closeness is measured by the number of 1-hop neighbors a node has. Second, QoS trust accounts for the capability of a node to complete a given mission. We consider *the energy level* and degree of *unselfishness* (or cooperativeness) to estimate the QoS trust level of a node. A node's trust value changes dynamically to account for trust decay over time due to node mobility or failure, as the trust chain becomes longer, as the node's energy level changes, and as the node becomes selfish or unselfish.

We define a node's trust level as a continuous real number in the range of [0,1], with 1 indicating complete trust, 0.5 ignorance, 0 complete distrust. The overall trust value is derived based on three trust components explaining the status of a node in terms of energy (probability of being alive with remaining energy $\leqslant$ energy threshold, T_{energy}), unselfishness (i.e., probability of being unselfish while forwarding packets), and closeness (i.e., number of 1-hop neighbors).

Below we describe how the trust value is calculated. Our trust metric reflects three components as mentioned above: unselfishness, energy, and closeness. The subjective trust evaluation of node i toward node j inherently hinges on the length of the trust chain between i and j. Specifically the trust value ($T_{i,j}^{n\text{-hop}}(t)$) of node j as evaluated by node i over a n-hop trust chain is given by:

$$T_{i,j}^{n\text{-hop}}(t) = \sum_{x \in X} w_x T_{i,j}^{n\text{-hop},x}(t) \tag{1}$$

Three trust components shown in Eq. (1) are weighted by w_x where the set x includes unselfishness, energy, and closeness.

Next we describe how the trust value of node j in component x as evaluated by node i, $T_{i,j}^{n\text{-hop},x}(t)$, is obtained. If the length of the trust chain separating node i from node j is not greater than the maximum length of a trust chain (i.e., n hops), node i can update node j's trust value at time t with both direct and indirect information collected. If node j cannot be found within n hops, node i relies on node j's past trust value with some decay considered. Reflecting these two cases, $T_{i,j}^{n\text{-hop},x}(t)$ is calculated by:

$$T_{i,j}^{n\text{-hop},x}(t) = \begin{cases} \beta T_{i,j}^{n\text{-hop},x}(t-\Delta t) + (1-\beta) T_{i,j}^{n\text{-hop,indirect-}x}(t) & \text{if } H(i,j) \leqslant n \\ e^{-\rho \Delta t} T_{i,j}^{n\text{-hop},x}(t-\Delta t) & \text{otherwise} \end{cases} \tag{2}$$

In Eq. (2), when node j is found within n hops from node i's location ($H(i,j) \leqslant n$ where $H(i,j)$ is the hop distance between nodes i and j), both direct and indirect information are used to derive the trust value of node j evaluated by node i. Otherwise, the trust value at time t is evaluated based on past trust information at time $t - \Delta t$ with the decay factor $e^{-\rho\ \Delta t}$ to consider the staleness where ρ is a constant to normalize the decay. Note that Eq. (2) is applied only when node j exists in the system. When node j does not exist in the system due to energy depletion, node j's trust value will drop to zero. In Eq. (2), β is used as a weight for the node's own information, that is, "self-information" based on the past experience using trust value at time $(t - \Delta t)$, and, conversely, $1 - \beta$ is the weight for indirect information using recommendations, that is, the "other-information."

The probability that node j is found within n hops from node i, denoted by $P_{i,j}^{n\text{-hop}}(t)$, can be computed by:

$$\begin{aligned} P_{i,j}^{n\text{-hop}}(t) &= \sum_{k=1}^{n} q_{i,j}^{k\text{-hop}} \quad \text{where } q_{i,j}^{k\text{-hop}}(t) \\ &= \sum_{(l,m)S} \left(P_i^{\text{loc}=l}(t) P_j^{\text{loc}=m}(t)\right) \end{aligned} \tag{3}$$

Here S is a set covering all (l,m) pairs with the distance between l and m being k hops away; $P_{i,j}^{n\text{-hop}}(t)$ is the cumulative probability that the hop distance between two nodes $\leqslant n$; $q_{i,j}^{k\text{-hop}}(t)$ is the probability that the hop distance between two nodes is equal to k; and $P_i^{\text{loc}=k}(t)$ is the probability that node i is located in area k.

Please cite this article in press as: J.-H. Cho, I.-R. Chen, On the tradeoff between altruism and selfishness in MANET trust management, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.004

Indirect information for trust component x at time t using a n-hop trust chain, $T_{i,j}^{n\text{-hop,indirect-}x}(t)$, in Eq. (2) is computed by:

$$T_{i,j}^{n\text{-hop,indirect-}x}(t) = \frac{\sum_{m\in S}(T_{i,\ldots,m}^{n\text{-hop,PR}}(t)T_{m,j}^{\text{direct-}x}(t))}{|S|} \quad (4)$$

In Eq. (4), S is the set of functional trust recommenders, that is, the set of 1-hop neighbors of node j that know about node j most. In Eq. (4), $T_{i,\ldots,m}^{n\text{-hop,PR}}(t)$ refers to the path reliability for the route between nodes i and m, computed by the product of direct unselfishness trust values of all pairwise intermediate nodes between nodes i and m along the path. This process reflects an incomplete transitivity of trust in MANETs. That is, trust decays as it propagates, or as the trust chain grows. Note that based on Jøsang et al. [31], we use referral trust with $T_{i,\ldots,m}^{n\text{-hop,PR}}(t)$ and functional trust with $T_{m,j}^{\text{direct-}x}(t)$ (discussed in Eq. (5)). Consequently, $T_{i,j}^{n\text{-hop,indirect-}x}(t)$ is derived based on direct trust relationships of all intermediate nodes between nodes i and j to ensure independence of trust values of intermediate nodes involved [31].

The trust value of node j in component x as evaluated by node i based on direct evidence observed by node i at time t, $T_{i,j}^{\text{direct-}x}(t)$, in Eq. (4) is obtained by:

$$T_{i,j}^{\text{direct-}x}(t) = \min\left[\frac{P_j^x(t)}{P_i^x(t)}, 1\right] \text{ where } T_{i,j}^{\text{direct-}x}(0) = 1 \quad (5)$$

In Eq. (5), we reflect the subjective characteristic of trust by dividing node j's trust in x ($P_j^x(t)$) by node i's trust in x ($P_i^x(t)$). We assume that all nodes are trustworthy with a trust value of 1 at time $t = 0$. We also assume that direct trust evaluation is close to actual status, so $P_i^x(t)$ for x = unselfishness or energy can be directly obtained from our SPN model output which yields actual node status, while the $P_i^x(t)$ value for x = closeness should be computed based on location information ($P_i^{\text{loc}} = l(t)$ where l indicates a particular area). When x = closeness, $P_i^{\text{closeness}}(t)$ refers to the degree of node i's average closeness toward any node at time t and is computed by:

$$P_i^{\text{closeness}}(t) = \frac{n_i^{\text{1-hop}}(t)}{n_i^{\text{max-hop}}(t)} \quad (6)$$

where $n_i^{\text{1-hop}}(t)$ is the number of 1-hop neighbors of node i at time t, and $n_i^{\text{max-hop}}(t)$ is the total number of nodes in the system except node i at time t. That is, $P_i^{\text{closeness}}(t)$ means the closeness of node i toward any node.

To assess the accuracy of "subjective" trust obtained from Eq. (1), we compare it against "objective" trust calculated based on the node's actual status. Specifically, the objective trust of node i is calculated by:

$$T_j^{\text{obj}}(t) = \sum_{x\in X} w_x P_j^x(t) \quad (7)$$

Here $P_j^x(t)$ is the "ground truth" status of node j in x at time t.

Dynamic trust formation by adjusting the weights associated with trust components to optimize application performance in response to dynamically changing conditions is an important research area [32,34], but is outside of the scope of the paper. For the purpose of achieving the goal of the paper, we have selected three trust components, namely, energy, unselfishness, and closeness, to reveal the tradeoff between altruistic behavior (i.e., providing high service availability) vs. selfish behavior (i.e., saving energy), and we have considered a mission scenario for which all trust components are weighted equally.

We apply a model-based analysis in this paper utilizing a SPN model to describe the behaviors of nodes following their mobility model (random movement), energy model (Section 2.4) and selfishness vs. altruism behavior model (Section 2.5) assumptions. The underlying model of the SPN model is a semi-Markov model which, after being solved, yields the probability that a node is in a particular state at time t. For example, node i is in area k at time t, $P_i^{\text{loc}=k}(t)$, is an output of the SPN model. The actual "ground truth" status of node j in component x at time t, $P_j^x(t)$, is also output of the SPN model, which can be used to calculate objective trust according to Eq. (7). We will describe our performance model later in detail in Section 3. Here we note that objective trust in Eq. (7) refers to trustworthiness mentioned in [31], representing the "objective" trust level. We use objective trust as a sanity check to ensure accuracy of our measured trust values based on Eqs. (1)–(6).

2.4. Energy model

In this section, we discuss the communication overheads of beaconing, group communication, status exchange, and rekeying operations in our protocol design in terms of message traffic generated (i.e., bits generated per second) and energy consumption rate per node for these operations. Since the application is a MANET group, rekeying and group communication packets are disseminated to legitimate members through hop-by-hop multicasting, while beaconing and status exchange packets are disseminated to only 1-hop neighbors based on our protocol design.

The energy model describes the amount of energy consumed when a node is in a particular state. It is an input to our trust management protocol. We associate the energy level of a node with its status in selfishness and group membership. Depending on the remaining energy, each node acts differently. The degree of energy consumption is also affected by the node's state. Thus, these parameters are interwoven and affect a node's lifetime significantly.

A GCS in MANETs must handle events such as beaconing, group communication, rekeying, and status exchange. In particular, after a status exchange event, trust evaluation towards 1-hop neighboring nodes as well as distant nodes may be performed. Each node may transmit its own status (e.g., information providing the trust values) as well as status of other nodes (i.e., trust values) on a trust chain. Recall that we use recommendations from 1-hop neighbors for trust evaluation.

We design the transmission packet format (bits) based on $[\text{HMAC}_{K_G}|\langle H|D\rangle_{K_G}]$ where the main message, encrypted by a group key K_G, consists of header H and data payload D. A hash-based message authentication code (HMAC) using a MAC key derived from K_G is used to ensure message

Please cite this article in press as: J.-H. Cho, I.-R. Chen, On the tradeoff between altruism and selfishness in MANET trust management, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.004

integrity and authentication. Typically the size of MAC is 128 or 160 bits in the case of MD5 or SHA-1 respectively [50]. This allows us to estimate energy consumption upon packet transmission and reception in our energy model.

The energy consumption per bit for transmission is estimated by [29]:

$$P_t(i,j) = \alpha_1 d(i,j) \tag{8}$$

where $d(i,j)$ is the distance between transmitter i and receiver j, v is the path-loss factor (typically, $2 \leqslant v \leqslant 6$), and α_1 is a distance-independent parameter. For simplicity, we use $\alpha_1 = 10^{-11}$ [29], and $d(i,j) = R$, the wireless radio range. Hence, we have $P_t = 10^{-11} * (R)^2$ for the energy consumption per bit at a transmitter, assuming $v = 2$. The energy consumption per second for data transmission by a node is given by:

$$P_{\text{send}} = P_t[A + \text{BN}_{\text{1-hop}}^{\text{unselfish}} + \text{CN}_{\text{1-hop}}^{\text{selfish}}] \tag{9}$$

The first term is for energy consumption for transmission initiated by a node where A represents bits generated per second covering beaconing, group communication, status exchange, and rekeying operations. The second term is for energy consumption for forwarding packets from unselfish 1-hop neighbors ($N_{\text{1-hop}}^{\text{unselfish}}$) where B represents bits generated per second, covering the messages for group communication, and rekeying operations to be disseminated to all group members using multicasting. Beaconing and status exchange messages are not required to be disseminated to all group members, so they are excluded from forwarding. The third term indicates the energy consumption for transmitting packets from selfish 1-hop neighbors ($N_{\text{1-hop}}^{\text{selfish}}$) who do not forward group communication packets received from others, with C representing bits generated per second for rekeying operations. We note that $N_{\text{1-hop}}^{\text{unselfish}}$ is set to the average number of 1-hop neighboring nodes, and $N_{\text{1-hop}}^{\text{selfish}}$ is set to zero in the first round of iterations of the SPN subnet based on the assumption that all neighbors are unselfish. From the second round of iterations, the estimates of $N_{\text{1-hop}}^{\text{unselfish}}$ and $N_{\text{1-hop}}^{\text{selfish}}$ obtained at the end of the previous round of iterations are used. Note that $N_{\text{1-hop}}^{\text{unselfish}}$ and $N_{\text{1-hop}}^{\text{selfish}}$ are time-averaged values; they reflect the average behavior of the system and can be estimated after the first round of iterations. Node i's $N_{i,\text{1-hop}}^{\text{selfish}}$ is calculated as:

$$N_{i,\text{1-hop}}^{\text{selfish}} = \frac{\sum_{t=0}^{\max}\sum_{k=1}^{N_{\text{area}}} P_i^{\text{loc}=k}(t)\sum_{y\in Y} L_{i,\text{selfish}}^{\text{loc}=y}(t)}{N_{\text{interval}}} \tag{10}$$

$$L_{i,\text{selfish}}^{\text{loc}=k}(t) = \sum_{j\in S, i\notin S} P_{j,\text{selfish}}^{\text{loc}=k}(t) \tag{11}$$

In Eq. (11), S includes all nodes' IDs except node i and $L_{i,\text{selfish}}^{\text{loc}=k}(t)$ is the number of selfish nodes in area k except for the case that node i is selfish in area k at time t. Similarly, $L_{i,\text{selfish}}^{\text{loc}=y}(t)$, where y is an element of Y that includes k location itself, north, south, west, and east of area k as the 1-hop neighbor areas, gives the number of 1-hop neighbor selfish nodes in areas in Y, max is the upper bound of time measured and N_{interval} is the number of time points. $P_i^{\text{loc}=k}(t)$ is the probability that node i is located in area k at time t. $P_{j,\text{selfish}}^{\text{loc}=k}(t)$ is the probability that node j is selfish and located at area k. Both $P_i^{\text{loc}=k}(t)$ and $P_{j,\text{selfish}}^{\text{loc}=k}(t)$ can be obtained from the SPN model output. $N_{i,\text{1-hop}}^{\text{unselfish}}$ is calculated by the average number of 1-hop neighbors minus $N_{i,\text{1-hop}}^{\text{selfish}}$. Henceforth, we omit the symbol i in $N_{i,\text{1-hop}}^{\text{unselfish}}$ and $N_{i,\text{1-hop}}^{\text{selfish}}$ for simplicity.

Assume that a node may leave the group voluntarily with rate μ and may rejoin the group with rate λ. Then, the probability that a node is in the group is $\lambda/(\lambda+\mu)$ and the probability that it is not is $\mu/(\lambda+\mu)$. Then, the rekeying interval T_{rekeying} is calculated as:

$$T_{\text{rekeying}} = 1/\Lambda_{J+L} \quad \text{where } \Lambda_{J+L} = \frac{2\lambda\mu}{\lambda+\mu} \tag{12}$$

where Λ_{J+L} is the aggregate join and leave rate in equilibrium.

The energy consumed in reception is typically less than that for transmission; we assume $P_r = P_t/2$ and do not consider energy consumed in idle listening. The energy consumed per second by each member node for packet reception from 1-hop neighbors is calculated by:

$$P_{\text{receive}} = P_r[\text{AN}_{\text{1-hop}}^{\text{unselfish}} + \text{DN}_{\text{1-hop}}^{\text{selfish}}] \tag{13}$$

where A is the same as in Eq. (9) and D represents bits received per second for beacon, status exchange, rekeying, and group communication messages for which the selfish 1-hop neighboring nodes transmit. In Eq. (13), the first term represents the energy consumed by receiving packets forwarded from healthy 1-hop neighbors ($N_{\text{1-hop}}^{\text{unsefish}}$) and the second term indicates the energy consumed by receiving packets forwarded from selfish 1-hop neighbors ($N_{\text{1-hop}}^{\text{selfish}}$).

In summary, the consumed energy of a node per second is:

$$P = P_{\text{send}} + P_{\text{receive}} \tag{14}$$

If a member node is selfish, it does not forward any packet from others but just transmits its own packets. The energy consumption per second for data transmission by a selfish node is given by:

$$P_{\text{send,selfish}} = P_t A \tag{15}$$

If a member node is selfish, the energy consumption per second for receiving packets is also P_{receive} since we assume all nodes are in promiscuous mode. Thus, the node will save $P_{\text{send}} - P_{\text{send,selfish}}$ energy by being selfish. Thus, the total energy consumption for a selfish node per second is:

$$P_{\text{selfish}} = P_{\text{send,selfish}} + P_{\text{receive}} \tag{16}$$

If a node is a non-member, it will only transmit and receive beacon messages. Thus, the energy consumption per second for a non-member is computed as:

$$\begin{aligned} P_{\text{non-member}} &= P_{\text{send.non-member}} + P_{\text{receive,non-member}} \\ &= E(P_t + P_r N_{\text{1-hop}}) \end{aligned} \tag{17}$$

Here $N_{\text{1-hop}}$ includes both $N_{\text{1-hop}}^{\text{unselfish}}$ and $N_{\text{1-hop}}^{\text{selfish}}$ since any node that is alive will disseminate beacon messages, and E indicates bits transmitted/received per second for a beacon message.

Please cite this article in press as: J.-H. Cho, I.-R. Chen, On the tradeoff between altruism and selfishness in MANET trust management, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.004

2.5. Selfishness vs. altruism behavior model

A selfishness vs. altruism behavior model describes the behavior of a node as it switches between selfish and altruistic behavior to balance its individual welfare vs. the system global welfare. It is an input to our trust management protocol. We derive a selfishness vs. altruism behavior model from the classic demand and pricing (DP) model in the field of economics [3,22]. Henceforth, we will refer it as the *DP behavior model*. In the literature, the DP model has been applied extensively to practical real-world scenarios in demand vs. resource consumption behavior in applications such as radio resource allocation in multimedia communication systems [41,43], distributed energy resource allocation in information and communication systems [42], and admission control for pricing optimization of multiple service classes in wireless networks [23]. We apply the DP model to describe the practical relationship between a node's selfish behavior vs. its energy status, the mission status, and the environment condition.

The basic formula to represent the relationship between demand and pricing in a market is given by:

$$\lambda^i = \gamma^i (v^i)^{-\varepsilon^i} \tag{18}$$

where λ^i is the demand arrival rate of service i and v^i is the pricing of service i while γ^i and ε^i are constants correlating to λ^i and v^i. Service demand is affected by pricing changes where the elasticity constant ε^i is a key determinant. Customers tend to purchase a product when they can afford to buy it or need it. If the increasing speed of demand is slower than that of pricing of a product, consumers are considered as inelastic to price changes. Conversely, if the increasing speed of demand is faster than that of pricing of a product, consumers are regarded as elastic to pricing changes. Usually the elasticity ε^i is greater than 1 in order to follow the general trend that a lower price increases consumer demand. The elasticity ε^i can be obtained from statistical data describing past market conditions.

We adopt the DP theory to model the behavior of a participating node particularly on whether it should behave selfishly or altruistically based on both individual benefit (i.e., saving energy) and global interest (i.e., serving tasks). To apply Eq. (18) to model the selfish behavior of a node, we use a transition T_SELFISH in our SPN model (discussed later in Section 3) to model a node's changing behavior from altruistic to selfish and vice versa. The transition rate for T_SELFISH indicates how often a node will switch from altruistic to selfish behavior and is modeled by:

$$\text{rate}(\text{T\_SELFISH}) = \frac{f(E_{\text{remain}}) f(M_{\text{difficulty}}) f(S_{\text{degree}})}{\text{T}_{\text{gc}}} \tag{19}$$

Applying the DP theory discussed in Eq. (18), we use $f(x) = \gamma x^{-\varepsilon}$ where a node is more likely to be selfish with large γ and small ε while it is less likely to be selfish with small γ and large ε. E_{remain} represents the level of current energy (mark(energy)), $M_{\text{difficulty}}$ is the difficulty level of a given mission where a higher number indicates a tougher mission with more workload, and S_{degree} is the degree of selfishness where a higher number refers to more selfishness. We define S_{degree} as the degree of selfish nodes to unselfish nodes among 1-hop neighbors. Note that when x in $f(x)$ is large, then a node is more likely to be altruistic. That is, when E_{remain}, $M_{\text{difficulty}}$ or S_{degree} is large, then a node tends to be altruistic because it has a sufficient level of energy, the mission is difficult, or few neighboring nodes are available to serve the mission. On the other hand, when a node has low energy, the mission is light-workload, or many altruistic neighbors are around, the node is more likely to be selfish so as to save energy to participate in mission execution. The DP theory is utilized to model a selfishness vs. altruism behavior scenario in which nodes attempt to achieve both individual benefit (i.e., saving energy) and global interest (i.e., serving tasks).

We use three different thresholds to order the degrees of these three environmental conditions. Thus, E_{remain}, $M_{\text{difficulty}}$, and S_{degree} are in the range of 1, 2, or 3. The multiplication by $1/T_{\text{gc}}$ is to consider an interval of disseminating a group communication packet where a node's selfishness can be observed. Eq. (19) implies the following physical meanings:

- $f(E_{\text{remain}})$: If a node has a higher level of energy, it is less likely to be selfish.
- $f(M_{\text{difficulty}})$: If a node is assigned a tougher mission, it is less likely to be selfish (so it would not risk mission failure).
- $f(S_{\text{degree}})$: If a node observes high selfishness among its 1-hop neighbors, it is less likely to be selfish (so it would not risk mission failure).

Similarly, we use a transition T_REDEMP in the SPN model (shown in Section 3.1) to model the redemption of a node changing its behavior from selfish to altruistic. The rate to transition T_REDEMP is modeled as:

$$\text{rate}(\text{T\_REDEMP}) = \frac{f(E_{\text{consumed}}) f(M_{\text{easiness}}) f(H_{\text{degree}})}{\text{T}_{\text{status}}} \tag{20}$$

where E_{consumed} is the level of consumed energy ($E_{\text{init}} - \text{mark(energy)}$), M_{easiness} is the easiness level of a given mission where a higher number indicates an easier mission with less workload, and H_{degree} is the degree of unselfishness where a higher number means more unselfishness of 1-hop neighbors. We define H_{degree} as the degree of unselfish nodes to selfish nodes among 1-hop neighbors. The redemption rate is high when a node has a sufficient energy, a difficult mission is given, or less healthy (or more selfish) nodes are available around the node, and vice versa, applying the same rationale in Eq. (19). A node is given a chance to be redeemed (from selfish to altruistic) in every revaluation period T_{status}, corresponding to the status exchange interval for trust evaluation. Eq. (20) carries the following physical meanings:

- $f(E_{\text{consumed}})$: If a node has consumed more energy, it is less likely to redeem itself. This means that if a node has low energy, it may want to further save its energy by remaining selfish.
- $f(M_{\text{easiness}})$: If a node is assigned to an easier mission, it is less likely to redeem itself (as this would not risk mission failure).

Please cite this article in press as: J.-H. Cho, I.-R. Chen, On the tradeoff between altruism and selfishness in MANET trust management, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.004

- $f(H_{\text{degree}})$: If a node observes high unselfishness among its 1-hop neighbors, it is less likely to redeem itself and may continue to stay selfish in order to save its energy (as this would not risk mission failure).

3. Performance model

3.1. Hierarchical modeling using SPN

We develop a mathematical model based on SPN techniques [37] to analyze a GCS with nodes switching between selfish and altruistic behavior based on the DP theory and identify design conditions under which the selfish vs. altruistic behaviors can be balanced. With the trust-based system lifetime and the mission success probability as our reliability metrics, we show that the DP behavior model outperforms one that only encourages altruistic behaviors. We use SPN as our modeling tool due to its efficient representation of a large number of states where the underlying models are semi-Markov models. We develop a hierarchical modeling technique to avoid state explosion problems and to improve solution efficiency for realizing and describing a large scale GCS.

We first develop a "node" SPN subnet to describe a single node's lifetime behavior. We assume that the operational area is a square-shaped area comprising $m \times m$ sub-grid areas with the width and height equal to the wireless radio range (R). Initially the location of each node is randomly distributed over the operational area based on uniform distribution. A node randomly moves to one of four locations in four directions (i.e., north, west, south, and east) in accordance with its mobility rate. The speed of each node is chosen from $[0,2)$ m/s based on uniform distribution at the beginning of network deployment, and is then fixed during its lifetime. The boundary grid areas are wrapped around (i.e., a torus is assumed) to reuse the operational area. The SPN subnet for node i computes the probability that node i is in a particular grid area j at time t. This information along with the information of other nodes' location information at time t provides actual status information about a node's n-hop neighbors at time t, which we will use to compute the "objective" trust metric. Since node movements are assumed to be independent, the probability that two nodes are in a particular location at time t is given by the product of the two individual probabilities. The node SPN subnet describes a node's lifetime behavior and can be used to obtain each node's status information (e.g., amount of energy left, unselfishness status, and closeness status) to derive the trust relationship with other nodes in the system. There are N such SPN subnets, one for each node in the network.

Iterative techniques are used for each node SPN subnet to obtain other nodes' information from other node SPN subnets since one subnet only describes one node's lifetime. In the first round of iterations, there is no information available about 1-hop neighbors, so it is assumed that each area has an equal number of nodes and all nodes are unselfish. In the second round of iterations, based on the information collected (e.g., number of unselfish or selfish 1-hop neighbors) from the first round, each node knows how many nodes are 1-hop neighbors that can directly communicate with it, and whether or not they are members of the GCS or selfish. A node also knows how many n-hop neighbors it has at time t. It then adjusts the status of 1-hop neighbors at time t with the output generated from the jth round of iterations as input to the $(j+1)$th round of iterations. This process continues until a specified convergence condition is met. The Mean Percentage Difference (MPD) is used to measure the difference between critical design parameter values, including the energy level, selfish probability, and closeness probability of a node at time t in two consecutive iterations. The iteration stops when the MPD is below 1% for all nodes in the system to assure accuracy. The calculation of the MPD of trust property x of node i is given by:

$$\text{MPD}_i^x = \frac{\sum_t^{\max} D_i^x(t)}{N_{\text{interval}}}; \quad D_i^x(t) = \frac{|x_i^{j+1}(t) - x_i^j(t)|}{x_i^j(t)} \tag{21}$$

where $x_i^j(t)$ indicates the value of trust property x of node i at time t in the jth round of iterations, max is the maximum time measured, and N_{interval} is the number of time points. We compute the MPD of trust property x including the energy level, selfish probability, and closeness probability of a node. The node SPN subnet after convergence yields actual status expressed in terms of the probabilities for various trust components (i.e., unselfishness, energy, and closeness) as output. Leveraging the SPN model output, we are able to calculate subjective and objective trust values as explained earlier in Section 2.3.

Fig. 1 shows the node SPN subnet. The subnet describes a node's mobility behavior, join and leave events (i.e., GCS membership status), energy consumption, and selfish behaviors with a redemption mechanism provided. Place *Location* holds the location ID (one of the $m \times m$ subareas each having a distinct location ID). If the current location ID is 3, there will be 3 "tokens" in *Location*. The transition T_LOCATION is triggered when a node moves to a randomly selected area in one of four different directions from its current location with the rate calculated as S_{init}/R based on an initial speed (S_{init}) and wireless radio range (R). For example, if a node moves downward from location 3 to location 8, then the number of tokens in *Location* is changed from 3 to 8 to reflect the location change. Hence, by examining the number of tokens in *Location*, we know a node's current location.

Place *Member* indicates whether a node is a member or not, with one token indicating yes and zero token indicating no. We assume that inter-arrival times of a node's join and leave requests are exponentially distributed with rates λ and μ, applying to transitions T_JOIN and T_LEAVE, respectively.

Place *Energy* represents the current energy level of a node. An initial energy level is assigned according to node heterogeneity information. In our analytical model, we randomly generate a number between 6 and 12 h of energy based on uniform distribution. A token representing an energy unit is taken out when transition T_ENERGY fires. The transition rate of T_ENERGY is adjusted on the fly based on a node's status: it is lower when a node becomes selfish to save energy or when a node changes its membership from a member to a non-member, following the energy con-

Please cite this article in press as: J.-H. Cho, I.-R. Chen, On the tradeoff between altruism and selfishness in MANET trust management, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.004

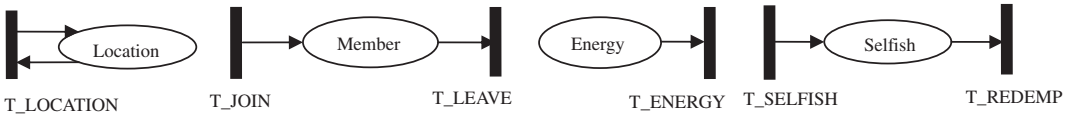

Fig. 1. Node SPN subnet for describing the behavior of a node.

sumption model explained in Section 2.4. We assume that T seconds will be taken to consume one energy token when a member node has no selfish 1-hop neighbors. We use our energy consumption model (see Section 2.4) for adjusting the time taken to consume one token in place *Energy* based on a node's status: a token is taken out of place *Energy* after T (i.e., $=(P \times T)/P$) seconds if the node is an unselfish member, $(P \times T)/P_{\text{selfish}}$ if it is a selfish member, and $(P \times T)/P_{\text{non-member}}$ if the node is a non-member. Therefore, depending on the node's status, its energy consumption rate is dynamically changed.

Place *Selfish* indicates whether a node is selfish or not, with one token in place *Selfish* representing it is selfish and zero token otherwise. If a node becomes selfish, a token goes to *Selfish* by triggering T_SELFISH. When a node becomes altruistic again, transition T_REDEMP is triggered. A node switches between selfish and altruistic following Eqs. (19) and (20). To model a compromised node which performs packet dropping attacks and stays selfish continuously, we disable T_REDEMP for a compromise node whose initial status is selfish, having a token in place *Selfish* from the beginning.

3.2. Calculation of trust

Subjective trust evaluation is performed by individual nodes at runtime. Essentially subjective trust is calculated by Eq. (1). Objective trust, on the other hand, is calculated by Eq. (7). Recall that objective trust is calculated based on actual status and is used as a baseline case against which accuracy is assessed. To apply Eqs. (1) and (7), we need to know node i's actual status in trust component x at time t (with x = energy, unselfishness or closeness), i.e., $P_i^{\text{energy}}(t)$, $P_i^{\text{unselfish}}(t)$ and $P_i^{\text{closeness}}(t)$. This can be achieved by means of a reward assignment technique described below. Specifically, the average value of a physical property at time t, $Z(t)$, is the state probability weighted sum of the values at various states, i.e.,

$$Z(t) = \sum_{j \in S} (r_j \text{Prob}_j(t)) \tag{22}$$

where $Z(t)$ represents the average value of a general physical property at time t, S is a set of states that meet particular conditions, $\text{Prob}_j(t)$ is the probability that the system is in state j at time t (which is output of our SPN model), and r_j is the "reward" or "value" assigned to the physical property at state j. The reward assignment technique allows us to compute a node's average energy level probability ($P^{\text{energy}}(t)$), unselfish probability ($P^{\text{unselfish}}(t)$), the probability of being in area k ($P^{\text{loc}=k}(t)$), $P^{\text{loc}=k}_{\text{unselfish}}(t)$ and $P^{\text{loc}=k}_{\text{selfish}}(t)$ needed in the computation of subjective trust (Eq. (1)) and objective trust (Eq. (7)). Also with knowledge of the probability of a node being in area k at time t ($P^{\text{loc}=k}(t)$) obtained above, we can compute $P_{i,j}^{n\text{-hop}}(t)$ from Eq. (3) as well as $P^{\text{closeness}}(t)$ from Eq. (5). Note that here we omit the subscript i (to refer to node i) for simplicity.

Table 1 specifies the conditions to be satisfied for states in set S in calculating $P^{\text{energy}}(t)$, $P^{\text{unselfish}}(t)$, $P^{\text{loc}=k}(t)$, $P^{\text{loc}=k}_{\text{unselfish}}(t)$, and $P^{\text{loc}=k}_{\text{selfish}}(t)$ as output of our SPN model. When the conditions specified are satisfied, a reward of 1 is assigned; 0 otherwise.

3.3. Calculation of trust-based reliability

We develop a computational procedure for assessing the mission reliability based on the trust level required for successful mission execution. The reliability of node j at time t, denoted by $R_j(t)$, is the probability that node j meets the required trust level for mission execution over time $[0,t]$, calculated as follows:

$$R_j(t) = \begin{cases} 0, & \text{if } T_j(t') = 0 \text{ for any } t' \leqslant t \\ E[T(t')] \text{ for } t' \leqslant t, & \text{otherwise} \end{cases}$$

where

$$T_j(t') = \begin{cases} 1, & \text{if } T_{i,j}^{n\text{-hop}}(t') \geqslant D_2 \\ 0, & \text{if } T_{i,j}^{n\text{-hop}}(t') < D_1 \\ T_{i,j}^{n\text{-hop}}(t')/D_2, & \text{otherwise} \end{cases} \tag{23}$$

In Eq. (23), t is the current time point and $t' \leqslant t$ is a past time point, D_1 is the drop dead trust level, and D_2 is the desired trust level for successful mission execution. The physical meaning is that if j's trust level is below the drop dead trust threshold (D_1) at any time during $[0,t]$ then $R_j(t)$ is zero; otherwise, $R_j(t)$ is the expected trust level scaled over the desired trust level (D_2). Knowledge of $R_j(t)$ thus can be obtained by node i (the commander node) based on its subjective trust toward node j ($T_{i,j}^{n\text{-hop}}(t')$ over $[0,t]$) according to Eq. (23) to decide if it should include node j as a group member to execute a mission assigned to ensure successful mission execution.

4. Numerical results and analysis

In this section, we present numerical results to compare subjective trust $T_{i,j}^{n\text{-hop}}(t)$ through Eq. (1), objective trust $T_j^{\text{obj}}(t)$ through Eq. (7) and the reliability of node j at time t, $R_j(t)$, through Eq. (23). We use SPNP as a tool to implement the SPN model developed and compute $T_{i,j}^{n\text{-hop}}(t)$, $T_j^{\text{obj}}(t)$ and $R_j(t)$ based on reward assignments as described in Section 3.2. Table 2 summarizes the default parameter values used in this paper.

In our case study, we assume that a mission requires the same level of importance in three dimensions of trust (i.e., energy, unselfishness, and closeness). The example

Please cite this article in press as: J.-H. Cho, I.-R. Chen, On the tradeoff between altruism and selfishness in MANET trust management, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.004

Table 1
Reward function.

Component	Reward returned based on conditions in S
$P^{\text{energy}}(t)$	mark(Energy) > 0
$P^{\text{unselfish}}(t)$	(mark(Member) > 0) & (*mark*(Selfish) == 0) &(*mark*(Energy) > 0)
$P^{\text{loc}=k}(t)$	(mark(Location) == k) &(mark(Member) > 0) & (*mark*(Energy) > 0)
$P^{\text{loc}=k}_{\text{unselfish}}(t)$	(mark(Member) > 0) & (*mark*(Selfish) == 0) & (mark(Energy) > 0) & (*mark*(Location) == k)
$P^{\text{loc}=k}_{\text{selfish}}(t)$	(mark(Member) > 0) & (*mark*(Selfish) > 0) & (mark(Energy) > 0) & (*mark*(Location) == k)

Table 2
Default parameter values used.

Parameter	Value	Parameter	Value	Parameter	Value
k_{recom}	3	N	150	D_1/D_2	0.5/0.85
R	250 m	T_{status}	600 s	w_X	1/3
λ	1/3600	T_{beacon}	120 s	γ	0.01
μ	1/14400	T	$60 * 60$ s	ε	2
β	0.8	S_{init}	(0,2) m/s	E_{init}	[6,12] h
T^{M1}_{gc}	600 s	T^{M2}_{gc}	360 s	T^{M3}_{gc}	120 s
Δt	600 s	ρ	1/3600	n (TC)	4

military mission scenario can be found in navigating and/or monitoring for locations or events on the enemy side where effective and efficient communications are vital to mission success [46]. In these types of missions, closeness, energy, and cooperativeness (unselfishness) are critical fundamental capabilities to make communication effective, leading to successful mission execution. Thus, we weigh all trust components equally, setting $w_X = 1/3$ to compute the overall trust based on Eq. (1). If a mission requires weapon or equipment capabilities for destroying buildings/bridges or rescuing personnel, a different set of trust dimensions can be added such as functionality (or diversity), and/or vertical mobility (e.g., airborne infantry) with a different level of importance [46]. What trust dimensions should be considered and how to weigh each trust dimension depend on the mission characteristics. Our work uses a weight parameter for each trust component so that the proposed trust metric can be generic and easily applicable to other mission scenarios.

To combine both direct evidence and indirect evidence to compute the overall trust, we weigh direct trust with $\beta = 0.8$ and indirect trust with $1 - \beta = 0.2$, at which the trust bias (i.e., the discrepancy between actual objective trust and measured subjective trust) is minimized at the optimal trust chain length of 4 (TC = 4). The reason direct trust (through observations) is weighted more than indirect trust (through recommendations) is that trust based on indirect evidence decays over *space* as it propagates along the trust chain especially as more intermediate nodes are on the trust chain. We control trust decay over *time* for a node with little interaction with others based on Eq. (2); the trust decay factor ρ is set to 1/3600 so that trust decay over time is limited by a ratio of $1 - (e^{-1})$ in 1 h.

The following three behavior models are being evaluated to test their effects on subjective trust and, through Eq. (23), on the mission success probability:

1. DP: This behavior model uses the demand and pricing (DP) theory to balance selfishness and altruism behavior of a node based on the environmental and operational conditions, as described in Section 2.5;
2. ALT: This is the behavior model where nodes are always altruistic by being cooperative (i.e., serving all requests) all the time; and
3. SELF: This is the behavior model where nodes are 50% selfish by dropping 50% of received packets.

Mission workload is regarded as one of most critical characteristics in military tactical environments [39,40]. In this work, we particularly consider mission workload in terms of packet transmission to reveal the tradeoff between altruism by cooperatively executing a mission vs. selfishness by energy conservation to prolong node lifetime, as we take both factors into consideration in our composite trust metric. Specifically, we consider three mission types (M1, M2, and M3) demanding different workloads, with M1 requiring the least workload while M3 requiring the most workload (i.e., M1 < M2 < M3). In Table 2, T^{M1}_{gc}, T^{M2}_{gc} and T^{M3}_{gc} are the service request inter-arrival times (for group communication) for M1, M2, and M3, respectively. These will be used in place of T_{gc} in Eq. (19) to calculate rate (T_SELFISH).

We first demonstrate that subjective trust obtained through Eq. (1) evolves over time and depends on the length of the trust chain (called TC for short). Fig. 2 shows the trust value of a trustee node as evaluated by a trustor node using the proposed trust metric calculation when the DP behavior model is used with the mission type being M1 demanding the lightest workload among three mission types considered. We aim to select an optimal TC to meet the acceptable trust accuracy level such that subjective trust does not exceed objective trust (OT) but is closest to OT. When subjective trust is higher than OT, it will reveal risk vulnerability by possible betrayal of collaborative parties [31]. From Fig. 2, we observe that using TC = 4 gives the most accurate subjective trust but reveals little risk from overestimating objective trust. This result can be applied to a mission execution situation in which the mission type is known (M1 as in Fig. 2) to set the maximum trust chain length (the n parameter) equal to the optimal TC length identified (e.g., 4 above in Fig. 2) so as to provide the best trust assessment accuracy without introducing risk due to overestimation.

Next we show the resulting subjective trust obtained under three different selfishness vs. altruism behavior models (DP, ALT, and SELF) when different mission types (M1, M2, and M3) are given. Figs. 3–5 graph the subjective trust value obtained vs. time under various behavior models when the mission types are M1, M2 and M3, respectively. We only show trust values above ignorance (0.5 in our trust scale [0,1]) over the time range [0,1000] min,

Please cite this article in press as: J.-H. Cho, I.-R. Chen, On the tradeoff between altruism and selfishness in MANET trust management, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.004

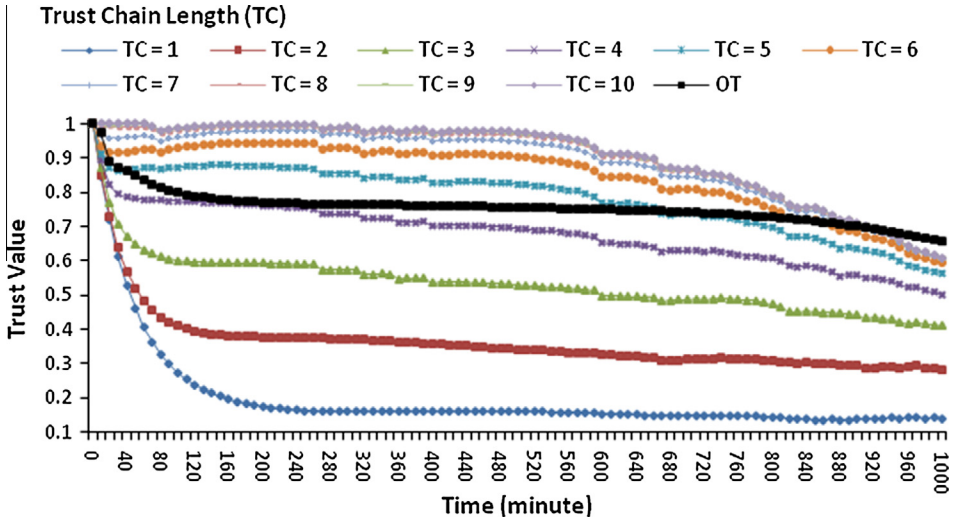

Fig. 2. Trust value vs. length of a trust chain (TC) over time: one node's evaluation toward another node.

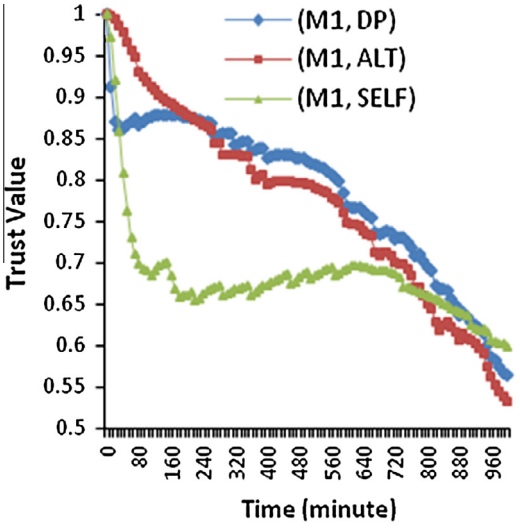

Fig. 3. Trust values obtained vs. time under various behavior models with mission type M1: one node's evaluation toward another node.

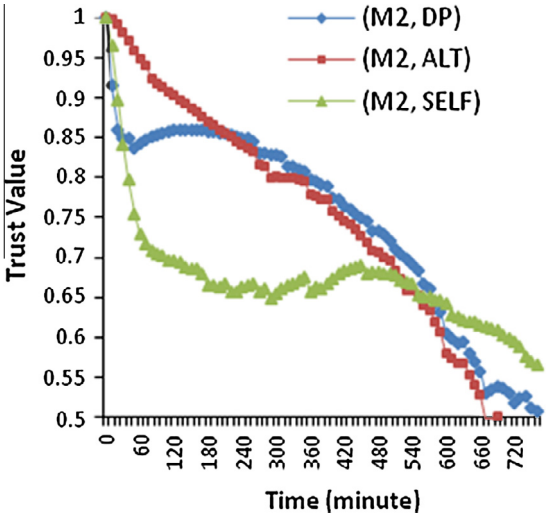

Fig. 4. Trust values obtained vs. time under various behavior models with mission type M2: one node's evaluation toward another node.

since trust less than ignorance is not meaningful for a node to be regarded as trustworthy for mission execution.

In Fig. 3, we see that when time is sufficiently small, say $t < 250$ min, ALT performs the best among the three behavior models. This is because in the beginning, most nodes have high energy, so unselfishness is the main factor among three trust components to determine trust. However, as time progresses (i.e., $t \geqslant 250$ min.), DP performs the best. This is because in ALT nodes always altruistically serve requests, so energy is easily depleted, thus resulting in a lower trust level after $t > 250$ min. When t is very large, $t \geqslant 950$ min in Fig. 3, SELF performs the best. This is because nodes in SELF have saved sufficient energy over a long period, compared with those in other models, so while nodes in DP or ALT consume most energy, nodes in SELF still maintain relatively high energy, resulting in a higher trust level. Note that in all three behavior models, trust is above ignorance (0.5) over the entire mission period, i.e., [0,1000] min.

Figs. 4 and 5 exhibit a similar trend as Fig. 3 except that the cross-over time point at which DP starts to perform better than ALT decreases as the mission type goes from M1 (Fig. 3) to M2 (Fig. 4) and M3 (Fig. 5). We see that the cross-over time point goes from 250 min. (Fig. 3) to 220 min. (Fig. 4) and 130 min. (Fig. 5). This is due to the fact that as we have a more difficult mission with a higher workload demand, nodes in ALT exhaust energy quickly. On the contrary, nodes in DP are able to exploit the tradeoff between selfishness (for their own welfare) and altruism (for global welfare) to save energy while providing cooperativeness when necessary. As a result, DP catches up with

Please cite this article in press as: J.-H. Cho, I.-R. Chen, On the tradeoff between altruism and selfishness in MANET trust management, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.004

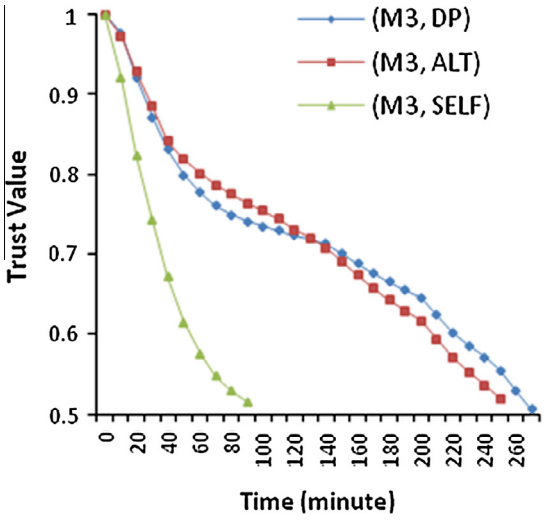

Fig. 5. Trust values obtained vs. time under various behavior models with mission level M3: one node's evaluation toward another node.

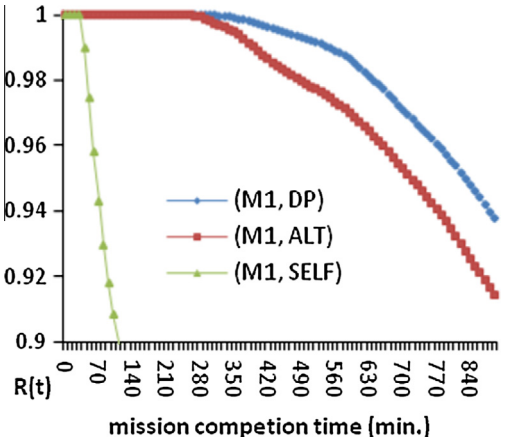

Fig. 7. A node's trust-based reliability $R(t)$ over time under M1 under various behavior models.

ALT after a shorter time span as the mission types goes from M1 to M2 and M3. In particular, we see from Fig. 5 that when the mission demands a high workload (i.e., under M3), SELF with 50% selfishness behavior provides the lowest trust level among three since 50% cooperativeness hurts both energy and cooperativeness, resulting in a low trust level under SELF, compared with that under ALT or DP. The effect is especially manifested as the mission time increases.

We can apply the results obtained here in two ways: (a) we can have some idea of the trust level obtainable under a behavior model (e.g., ALT) for design decision making; and (b) we can decide the mission execution time period such that trust is above a minimum threshold trust level (e.g., D2) before the mission execution period is expired.

In Fig. 6, we show the probability of a node's unselfishness under three behavior models and three mission types. We observe that as the mission's workload increases (i.e., from M1 to M2 and M3), a node's unselfishness trust in DP is not significantly different from the one in ALT. This is because a node in DP autonomously adjusts its selfishness vs. altruism behavior based on environmental and operational conditions including its own energy level, other nodes' selfishness status, and the mission type. For a highly demanding mission (say M3), nodes in DP will tend to be altruistic to serve other nodes' requests as much as ALT does for global welfare. Thus, we do not see much discrepancy in unselfishness between DP and ALT under M3. However, for a less demanding mission (say M1), nodes in DP tend to be somewhat selfish for individual welfare without compromising global welfare. Thus, we observe there is a subtle difference in unselfishness between DP and ALT under M1, i.e., ALT's unselfishness (or cooperativeness) trust is higher than DP.

Based on Eq. (23), we test the effect of the selfishness vs. altruism behavior model on a node's trust-based reliability $R(t)$ under three mission types (M1, M2, and M3) with $D_1 = 0.5$ and $D_2 = 0.85$. Figs. 7–9 graph $R(t)$ vs. time under three behavior models for mission types M1, M2 and M3, respectively. Here we omit the subscript j in $R_j(t)$ for simplicity. When the mission has a relatively low degree of dif-

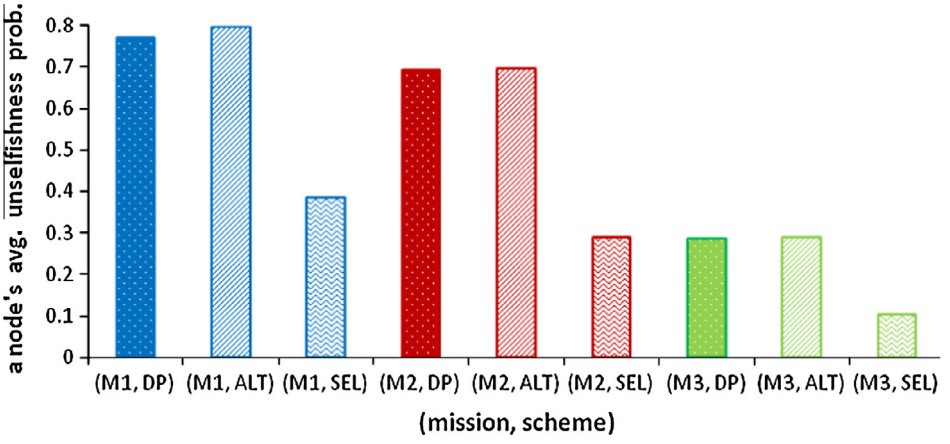

Fig. 6. A node's unselfishness trust under various behavior models and mission types.

Please cite this article in press as: J.-H. Cho, I.-R. Chen, On the tradeoff between altruism and selfishness in MANET trust management, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.004

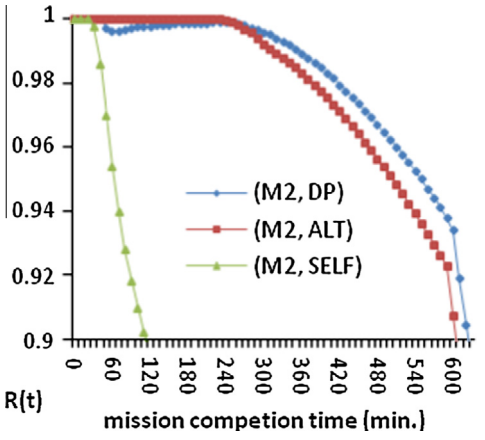

Fig. 8. A node's trust-based reliability $R(t)$ over time under M2 under various behavior models.

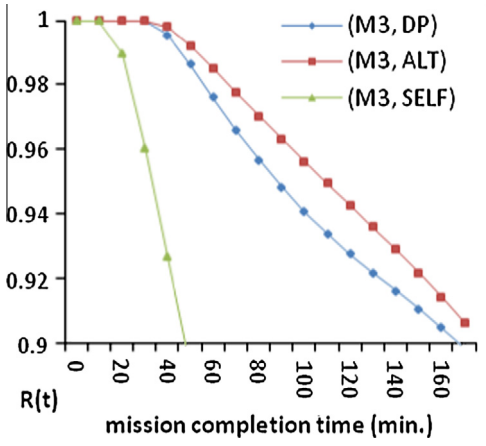

Fig. 9. A node's trust-based reliability $R(t)$ over time under M3 under various behavior models.

ficulty with a low workload (i.e., M1 or M2), the benefit of DP in terms of $R(t)$ is pronounced. This is because DP can best balance selfishness vs. altruism behavior to gain a trust level above D2 compared with the other two extreme behavior models (ALT and SELF). As we go from M1 to M2 and M3, a node in DP for global welfare becomes more altruistic to serve requests received, thus mimicking the behavior of an altruistic node. Moreover, as the mission workload increases (from M1 to M3), we observe that ALT even performs better than DP because unlike in ALT, a node in DP is not 100% altruistic and its unnecessary selfish behavior decreases the trust level needed for achieving M3. Among all, SELF is the worst in terms of $R(t)$ because 50% selfishness behavior achieves little trust in terms of both energy and cooperativeness properties, the effect of which is especially pronounced for a mission (M3) demanding a high workload. Note that here we only graph the results for which $R(t)$ is above 0.9 as presumably only a node with reliability above 0.9 is qualified for mission execution.

Existing work in trust/reputation systems [13–19] focused on cooperativeness or altruism which is considered

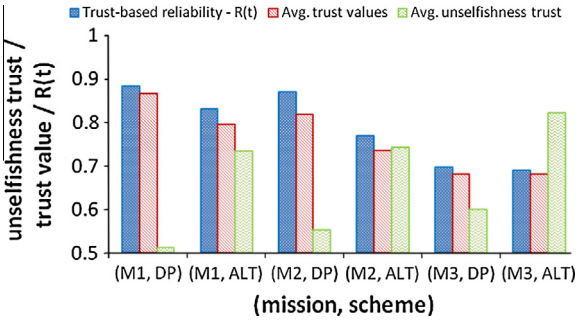

Fig. 10. A comparative performance analysis of DP vs. ALT over all mission scenarios.

as the global welfare of a system. Thus, we consider ALT representing existing schemes and compare it against our DP behavior scheme. Fig. 10 compares ALT with DP in the mission reliability, the overall trust, and the unselfishness trust, covering all mission scenarios. We observe that although ALT dominates DP in altruism (unselfishness), DP outperforms ALT in both the overall trust and the mission reliability, especially when the mission is less difficult to execute (i.e., M1). This is because altruism (unselfishness) does not guarantee mission success. Excessive altruism quickly drains energy, thus shortening a node's lifetime that leads to its incapacitation to execute the mission. We conclude that it is not necessarily always desirable to encourage cooperative behavior.

Our work identifies the intelligent altruism vs. selfishness behavior of a node modeled based on the DP theory to maximize the mission reliability and the overall trust over time. In practice, given knowledge of a team composition (e.g., a mobile group coalition comprising several nodes following the DP behavior model) for accomplishing a mission, one can parameterize ε and γ for modeling selfishness vs. altruism behaviors. Then, given knowledge of node selfishness vs. altruism behaviors for a mission with a certain degree of difficulty (M1, M2 or M3) as input, one can use the model-based analysis methodology presented in the paper to assess trust vs. time, and $R_j(t)$ vs. time, and, consequently, the mission success probability.

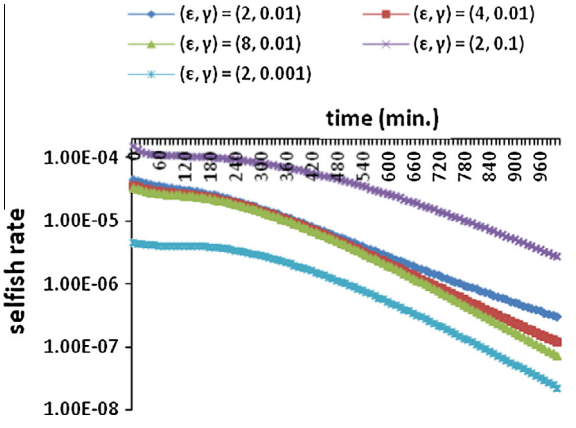

Fig. 11. Sensitivity of selfish rate as (ε, γ) varies.

Please cite this article in press as: J.-H. Cho, I.-R. Chen, On the tradeoff between altruism and selfishness in MANET trust management, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.004

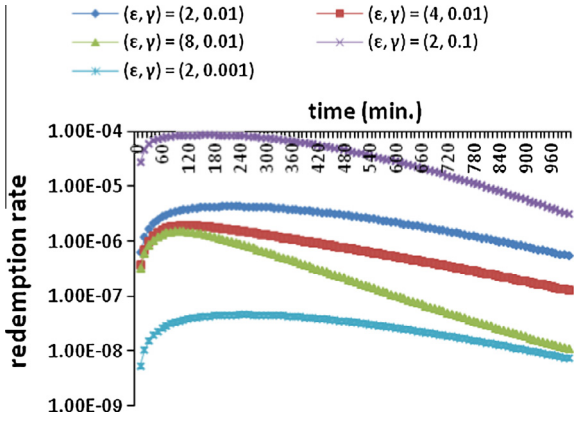

Fig. 12. Sensitivity of redemption rate as (ε,γ) varies.

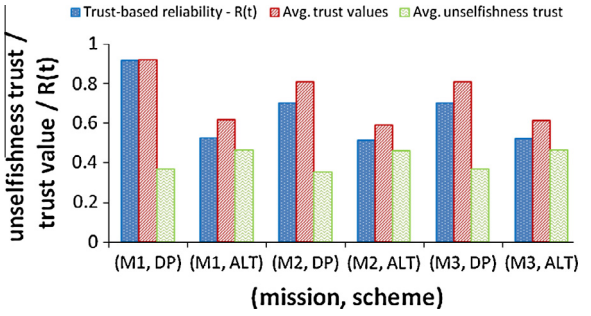

Fig. 14. A comparative performance analysis of DP vs. ALT over all mission scenarios in the presence of 20% compromised nodes.

To show worthiness and usefulness of our analysis methodology, we conduct sensitivity analyses of the analysis results (unselfishness trust, overall trust, and mission success reliability) with respect to ε and γ in Eqs. (19) and (20) in the DP behavior model. These two parameters control the change rate of selfishness and altruism.

Figs. 11 and 12 show the sensitivity of the altruistic to selfish switch rate (called selfish rate in our SPN model), and the selfish to altruistic switch rate (called redemption rate in our SPN model), respectively, with respect to (ε,γ), assuming that the same (ε,γ) is used for both rates. We observe that as either ε or γ increases, the selfish rate (or redemption rate) also increases. The impact of γ is more significant than the impact of ε, implying that γ is a more important parameter of the DP behavior model than ε in modeling a node's altruism vs. selfishness behavior.

Fig. 13 vividly shows the resulting unselfishness trust, overall trust and mission reliability with ε and γ given as input. We again observe that γ has a higher impact than ε on the unselfishness trust and overall trust. As expected, the mission reliability increases as the overall trust increases. However, we observe that the mission reliability decreases as node altruism (unselfishness) increases. This verifies our hypothesis that cooperative behavior does not always increase system performance as high service availability can unnecessarily shorten node lifetime.

Finally, we analyze the sensitivity of the results with respect to the presence of compromised nodes which perform packet dropping attacks and stay selfish continuously. Our intent is to reveal the impact of compromised nodes on a node's self-adapting altruistic vs. selfish behavior adjustment decision, and if the results obtained are resilient to an increasing compromise node population.

Fig. 14 shows the performance comparison of DP and ALT schemes in the mission reliability, the overall trust, and the unselfishness trust in the presence of 20% compromised nodes in the network for the beginning 2 h of the mission period. In Fig. 14, we observe a similar trend as exhibited in Fig. 10, i.e., ALT performs better than DP in altruism (unselfishness), and DP outperforms ALT in both the overall trust and the mission reliability. However unlike Figs. 10 and 14 show that while the dominance of DP over ALT remains, the dominance is less sensitive to the mission difficulty level (i.e., from M1 to M3). The reason is that unselfish behavior adjustment is mainly controlled by the unselfish neighboring node population around each node. Therefore, in the presence of more unselfish nodes around each node, there is less room for dynamic unselfish behavior adjustment.

Fig. 15 analyzes the impact of the % of compromised nodes in the system on the performance of the DP and ALT schemes for the beginning 2 h of the mission period. We observe that by means of self-adapting altruistic vs. selfish behavior control, DP outperforms ALT in mission

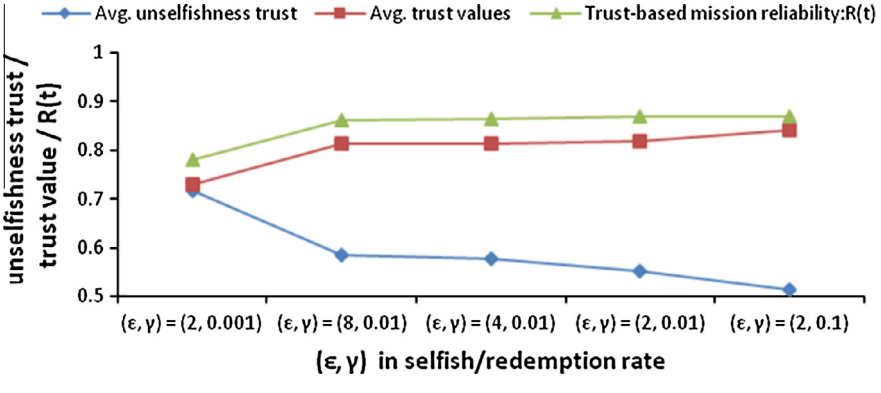

Fig. 13. Impact of (ε,γ) on unselfishness trust, overall trust and mission reliability.

Please cite this article in press as: J.-H. Cho, I.-R. Chen, On the tradeoff between altruism and selfishness in MANET trust management, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.004

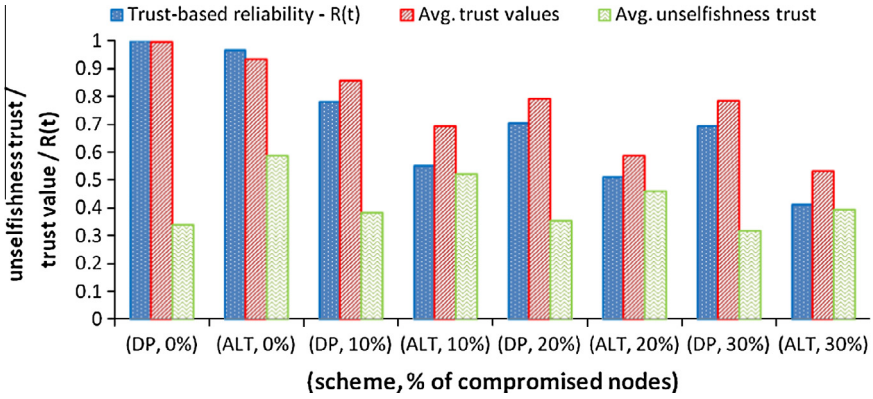

Fig. 15. A comparative performance analysis of DP vs. ALT with % compromised varying in [0–30%].

reliability over a wide range of hostility conditions (with 33% compromised nodes being the maximum since a system subject to Byzantine failure [51] will fail when the percentage of compromises nodes exceeds 33%). Moreover, the dominance widens as the hostility increases from 0% to 30% compromised nodes. This demonstrates the effectiveness of self-adapting altruistic vs. selfish behavior adjustment as the hostility increases in response to dynamically changing conditions.

5. Conclusions and future work

In this paper, we developed and analyzed a trust management protocol for a mission-driven GCS in MANETs based on the demand and pricing (DP) theory to model node selfishness or altruism behaviors to balance individual welfare (i.e., saving energy) vs. global welfare (i.e., serving tasks and completing the mission). We developed a probability model based on SPN to describe the behaviors of a large scale GCS operating under the proposed trust management protocol in MANETs. The results showed that the DP behavior model exploiting the tradeoff between selfishness vs. altruism outperforms one that only encourages altruistic behaviors, or one that only encourages selfishness, especially when the mission demands a light to medium workload. We attribute the superiority of the DP behavior model to its ability to explore the tradeoff between energy saved due to selfishness vs. quick energy drainage due to altruism for mission execution.

Our proposed behavior model based on DP theory can be applicable to resource-restricted environments with a large number of nodes. For example, Kumer et al. [47] addressed security requirements for health monitoring systems using a large number of medical Telos-motes. Polastre et al. [48] presented Telos, a low power wireless sensor module (“mote”) where one goals is to minimize power consumption. In addition, Kioumars and Tang [49] proposed a wireless sensor developed based on the ATmega micro-controller and the XBee protocol for health monitoring that incurs low power consumption. Our proposed DP model can contribute further to achieving both low power consumption and reliable service provision based on the balance between altruism and selfishness in response to network dynamics.

As future work, we plan to develop a more sophisticated mission model considering the effect of mission attributes such as the risk, deadline, and specific workload requirements. In addition, we plan to investigate a hybrid scheme that allows the system with fuzzy failure criteria [45] to adaptively switch between DP and ALT trust management to maximize the system reliability for mission execution and to achieve survivability. In this paper we have adopted a random mobility model for node movements. This yields the “closeness” trust component ineffective in our trust management protocol. In the future, we plan to enhance our analysis with mobility models or traces that can better describe node movements of mission group.

Acknowledgements

This material is based upon work supported in part by the U. S. Army Research Laboratory and the U. S. Army Research Office under Contract number W911NF-12-1-0445. This research was also partially supported by the Department of Defense (DoD) through the office of the Assistant Secretary of Defense for Research and Engineering (ASD (R&E)). The views and opinions of the author(s) do not reflect those of the DoD nor ASD (R&E).

References

[1] R.W. Thomas, D.H. Friend, L.A. DaSilva, A.B. MacKenzie, Cognitive networks: adaptation and learning to achieve end-to-end performance objectives, IEEE Communications Magazine, Topics in Radio Communications 44 (12) (2006) 51–57.
[2] C.H. Papadimitriou, Algorithms, Games, and the Internet, in: Proc. 33rd Annual ACM Symposium on Theory of Computing, Hersonissos, Crete, Greece, 6–8 July 2001, pp. 749–753.
[3] K.E. Case, R.C. Fair, Principles of Economics, fifth ed., Prentice-Hall, 1999.
[4] R. Falcone, C. Castelfranci, Social Trust: A Cognitive Approach, Trust and Deception in Virtual Societies, Kluwer Academic Publishers, 2001. pp. 55–90.
[5] V.V. Das, IP-based credit mobile ad-hoc networks, in: Int'l Conf. on Computational Intelligence and Multimedia Applications, vol. 4, 13–15 December 2007, pp. 453–457.
[6] D. Djenouri, N. Ouali, A. Mahmoudi, N. Badache, Random feedbacks for selfish nodes detection in mobile ad hoc networks, Lecture Notes in Computer Science: Operations and Management in IP-Based Networks 3751 (2005) 68–75.

[7] F. Kargl, A. Klenk, S. Schlott, M. Weber, Advanced detection of selfish or malicious nodes in ad hoc networks, Lecture Notes in Computer Science: Security in Ad Hoc and Sensor Networks 3313 (2005) 152–165.
[8] Y. Wang, V.C. Giruka, M. Singhal, Truthful multipath routing for ad hoc networks with selfish nodes, Journal of Parallel and Distributed Computing 68 (6) (2008) 778–789.
[9] D. Zhao, Access control in ad hoc networks with selfish nodes, Wireless Communications and Mobile Computing 6 (6) (2006) 761–772.
[10] L. Yan, S. Hailes, Designing incentive packet relaying strategies for wireless ad hoc networks with game theory, IFIP Int'l Federation for Information Processing: Wireless Sensor and Actor Networks II 264 (2008) 137–148.
[11] H. Miranda, L. Rodrigues, Friends and foes: preventing selfishness in open mobile ad hoc networks, in: Proc. 23rd Int'l Conf. on Distributed Computing Systems Workshops, 19–22 May 2003, pp. 440–445.
[12] Q. Zhang, D.P. Agrawal, Impact of selfish nodes on route discovery in mobile ad hoc networks, IEEE Global Telecommunications Conference 5 (2004) 2914–2918. 29 November–3 December.
[13] M.T. Refaei, S. Vivek, L. DaSilva, M. Eltoweissy, A Reputation-based mechanism for isolating selfish nodes in ad hoc networks, in: Proc. 2nd Annual Int'l Conf. on Mobile and Ubiquitous Systems: Networking and Services, 17–21 July 2005, pp. 3–11.
[14] Q. He, D. Wu, P. Khosla, SORI: a secure and objective reputation-based incentive scheme for ad-hoc networks, IEEE Wireless Communications and Networking Conference 2 (2004) (2004) 825–830.
[15] N. Pisinou, T. Ghosh, K. Makki, Collaborative trust-based secure routing in multi-hop ad hoc networks, in: Proc. 3rd Int'l IFIP-TC06 Networking Conf., Lecture Notes in Computer Science: Networking 2004, Athens, Greece, vol. 3042, 9–14 May 2004, pp. 1446–1451.
[16] S. Soltanali, S. Pirahesh, S. Niksefat, M. Sabaei, An efficient scheme to motivate cooperation in mobile ad hoc networks, in: Int'l Conf. on Networking and Services, Athens, Greece, 19–25 June 2007, pp. 98–103.
[17] M.E.G. Moe, B.E. Helvik, S.J. Knapskog, TSR: trust-based secure MANET routing using HMMs, in: Proc. 4th ACM Symposium on QoS and Security for Wireless and Mobile Networks, Vancouver, British Columbia, Canada, 27–28 October 2008, pp. 83–90.
[18] W.J. Adams, G.C. Hadjichristofi, N.J. Davis, Calculating a node's reputation in a mobile ad hoc network, in: Proc. 24th IEEE Int'l Performance Computing and Communications Conf., Phoenix, AX, 7–9 April 2005, pp. 303–307.
[19] P.B. Velloso, R.P. Laufer, D. Cunha, O.C.M.B. Duarte, G. Pujolle, Trust management in mobile ad hoc networks using a scalable maturity-based model, IEEE Transactions on Network and Service Management 7 (3) (2010) 172–185.
[20] J.H. Cho, A. Swami, I.R. Chen, Modeling and analysis of trust management for cognitive mission-driven group communication systems in mobile ad hoc networks, in: 2009 IEEE/IFIP Int'l Symposium on Trusted Computing and Communications, vol. 2, Vancouver, Canada, August 2009, pp. 641–650.
[21] P. Marbach, Y. Qiu, Cooperation in wireless ad hoc networks: a market-based approach, IEEE/ACM Transactions on Networking 13 (6) (2005) 1325–1338.
[22] M. Aldebert, M. Ivaldi, C. Roucolle, Telecommunications demand and pricing structure: an economic analysis, Telecommunication Systems 25 (1–2) (Jan. 2004) 89–115.
[23] O. Yilmaz, I.R. Chen, Utilizing call admission control for pricing optimization of multiple service classes in wireless cellular networks, Computer Communications 32 (2) (2009) 317–323.
[24] P. Rappaport, J. Alleman, L.D. Taylor, Household demand for wireless telephony: an empirical analysis, in: Proc. 31st Annual Telecommunications Policy Research Conf., Arlington, VA, September 2003.
[25] M. Li, E. Kamioka, S. Yanada, Pricing to stimulate node cooperation in wireless ad hoc networks, IEICE Transactions on Communications E90-B (7) (2007) 1640–1650.
[26] Y. Xi, E.M. Yeh, Pricing, competition, and routing for selfish and strategic nodes in multi-hop relay networks, in: INFOCOM 2008, 27th Conf. on Computer Communications, 13–18 April 2008, pp. 1463–1471.
[27] K. Chen, Z. Yang, C. Wagener, K. Nahrstedft, Market models and pricing mechanisms in a multihop wireless hotspot network, in: 2nd Annual Int'l Conf. on Mobile and Ubiquitous Systems: Networking and Services, 17–21 July 2005, pp. 73–82.
[28] L. Capra, Toward a human trust model for mobile ad-hoc networks, in: Proc. 2nd UK-UbiNet Workshop, 5–7 May 2004, Cambridge University, Cambridge, UK.
[29] A. Kansal, A. Ramamoorthy, M.B. Srivastava, G.J. Pottie, On sensor network lifetime and data distortion, in: Int'l Symposium on Information Theory, Adelaide, South Australia, 4–9 September 2005, pp. 6–10.
[30] J. Golbeck (Ed.), Computing with Social Trust, Human-Computer Interaction Series, Springer, 2009.
[31] A. Jøsang, S. Pope, Semantic constraints for trust transitivity, in: Proc. 2nd Asia-Pacific Conf. on Conceptual Modeling, Newcastle, Australia, 2005.
[32] J.H. Cho, A. Swami, I.R. Chen, Modeling and analysis of trust management protocols: altruism versus selfishness in MANETs, in: M. Nishigaki, A. Jøsang, Y. Murayama, S. Marsh (Eds.), 4th IFIP Int'l Conf. on Trust Management, Morioka, Japan, 14–18 June 2010; Trust Management IV, IFIP Advances in Information and Communication Technology, Springer, 2010, vol. 321, pp. 141–15.
[33] S. Marti, T. Giuli, K. Lai, M. Baker, Mitigating routing misbehavior in mobile ad hoc networks, in: Proc. 6th Annual ACM/IEEE Mobile Computing and Networking, Boston, MA, August 2000, pp. 255–265.
[34] F. Bao, I.R. Chen, M. Chang, J.H. Cho, Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection, IEEE Transactions on Network and Service Management 9 (2) (2012) 169–183.
[35] C.J. Fung, J. Zhang, I. Aib, R. Boutaba, Dirichlet-based trust management for effective collaborative intrusion detection networks, IEEE Transactions on Networks and Service Management 8 (2) (2011) 79–91.
[36] J.H. Cho, A. Swami, I.R. Chen, A survey of trust management in mobile ad hoc networks, IEEE Communications Surveys and Tutorials 13 (4) (2011) 562–583.
[37] G. Ciardo, J. Muppala, K. Trivedi, SPNP: stochastic petri net package, in: 3rd Int'l Workshop on Petri Nets and Performance Models, December 1989, pp. 142–151.
[38] M. Steiner, G. Tsudik, M. Waidner, Diffie-Hellman key distribution extended to group communication, in: Proc. 3rd ACM Conf. on Computer and Communications Security, New Delhi, India, January 1996, pp. 31–37.
[39] M.J. Skinner, P.A. Simpson, Workload Issues in Military Tactical Airlift, vol. 12, no. 1, 2002, pp. 79–93.
[40] Military Missions: Strategic Concept, US Army Corps of Engineers, Department of the Army, January 2012.
[41] A. Rad, V. Wong, V. Leung, Two-fold pricing to guarantee individual profits and maximum social welfare in wireless access networks, in: IEEE Global Telecommunications Conf., 2008, pp. 1–6.
[42] P. Nyeung, J. Ostergaard, Information and communications systems for control-by-price of distributed energy resources and flexible demand, IEEE Transactions on Smart Grid 2 (2) (2011) 334–341.
[43] M. Blomgren, J. Hultell, Demand-responsive pricing in open wireless access markets, in: IEEE 65th Vehicular Technology Conf., 2007, pp. 2990–2995.
[44] M. Heissenbüttel, T. Bruaun, T. Bernoulli, W. Walchli, BLR: beacon-less routing algorithm for mobile ad-hoc networks, Computer Communications 27 (2003) 1076–1086.
[45] F.B. Bastani, I.R. Chen, T. Tsao, Reliability of systems with fuzzy-failure criterion, in: Annual Reliability and Maintainability Symposium, Anaheim, CA, USA, January 1994, pp. 442–448.
[46] E.S. Tollefson, M.J. Kwinn, P.G. Martin, G.G. Boylan, B.L. Foote, Simulation modeling requirements for determining soldier tactical mission system effectiveness, in: Proc. 2004 Winter Simulation Conf., vol. 1, 2004.
[47] P. Kumar, Y.-D. Lee, H. Lee, Secure health monitoring using medical wireless sensor networks, in: 6th Int'l Conf. on Networked Computing and Advanced, Information Management, 2010, pp. 491–494.
[48] J. Polastre, R. Szewczyk, D.E. Culler, Telos: enabling ultra-low power wireless research, in: 4th Int'l Symposium on Information Processing in Sensor, Networks, 2005, pp. 364–369.
[49] A.H. Kioumars, L. Tang, ATmega and XBee-based wireless sensing, in: 5th Int'l Conf. on Automation, Robotics and Applications, 2011, pp. 351–356.
[50] H. Krawczyk, M. Bellare, R. Canetti, Request for Comments (RFC)-2104, February 1997, HMAC: Keyed-Hashing for Message Authentication, Network Working Group.
[51] F.C. Gärtner, "Byzantine Failures and Security: Arbitrary is Not (always) Random", Swiss Federal Institute of Technology (EPFL) School of Computer and Communication Sciences, Technical, Report IC/2003/20, 2003.

Please cite this article in press as: J.-H. Cho, I.-R. Chen, On the tradeoff between altruism and selfishness in MANET trust management, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.004

Jin-Hee Cho received the BA from the Ewha Womans University, Seoul, Korea and the MS and PhD degrees in computer science from the Virginia Tech. She is currently a computer scientist at the U.S. Army Research Laboratory (USARL), Adelphi, Maryland. Her research interests include wireless mobile networks, mobile ad hoc networks, sensor networks, secure group communications, group key management, network security, intrusion detection, performance analysis, trust management, cognitive networks, social networks, dynamic networks, and resource allocation. She is a member of the IEEE and ACM.

Ing-Ray Chen received the BS degree from the National Taiwan University, Taipei, Taiwan, and the MS and PhD degrees in computer science from the University of Houston. He is a professor in the Department of Computer Science at Virginia Tech. His research interests include mobile computing, wireless systems, security, trust management, data management, real-time intelligent systems, and reliability and performance analysis. Dr. Chen currently serves as an editor for *IEEE Communications Letters*, *IEEE Transactions on Network and Service Management*, *Wireless Personal Communications*, *Wireless Communications and Mobile Computing*, *The Computer Journal*, *Security and Network Communications*, and *International Journal on Artificial Intelligence Tools*. He is a member of the IEEE and ACM.

Please cite this article in press as: J.-H. Cho, I.-R. Chen, On the tradeoff between altruism and selfishness in MANET trust management, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.004